GOOGLE CO-MARKETING AGREEMENT

This co-marketing agreement ("**Agreement**") is effective as of the Effective Date and is entered into by Google and Partner.

"**Partner**"	**Full legal name:**	City of Helsinki (Helsingin kaupunki)
	Country of Incorporation:	Finland
	Address for Legal Notices: **Postal address (if different):**	City of Helsinki P.O.Box 20 00099 CITY OF HELSINKI
	Email address:	helsinki.kirjaamo@hel.fi
"**Google**"	**Full legal name:**	Google Finland Oy
	Country of Incorporation:	Finland
	Address for Legal Notices and Postal address:	Mannerheimintie 12 B 00100 Helsinki Attn: Legal Department
	Email address:	legal-notices@google.com
"**Effective Date**"	The date of last signature of this Agreement.	
"**Campaign Period"**	From 1st September 2019 until 31st March 2020, unless this Agreement is terminated earlier in accordance with the provisions herein.	
"Term"	This Agreement will start on the Effective Date and continue until 31st March 2020.	

1. **Definitions**.

1.1 "**Brand Features**" means trade names, trade and service marks, logos and other distinctive brand features of the applicable party.

1.2 **"Confidential Information"** means information that one party (or an affiliate) discloses to the other party under this Agreement, and that is marked as confidential or would normally be considered confidential information under the circumstances. It does not include information that is independently developed by the recipient, is rightfully given to

the recipient by a third party without confidentiality obligations, or becomes public through no fault of the recipient.

1.3 "**Content**" means any content that either party provides in connection with the Campaign including data, images, video, software or other materials as listed in Attachment B.

1.4 "**Campaign Marketing**" means any and all marketing or promotion by one or both parties of the Campaign, including as set out in Attachment A.

1.5 "**Campaign Materials**" means any and all marketing and promotional materials developed by Partner, Google or either parties subcontractors, including as set out in Attachment A.

1.6 "**Campaign Properties**" means any platform used to distribute or display the Campaign Materials which may include but will not be limited to a website.

1.7 "**Deliverables**" means any work product (including Campaign Materials) provided by either party as part of its joint effort to create and deliver the Campaign, as set out in this Agreement.

1.8 **"GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

1.9 **"Google Provided Content"** means the Content provided by Google as listed in Attachment B.

1.10 "**Intellectual Property***"* or "**IP**" means anything protectable as an Intellectual Property Right.

1.11 "**Intellectual Property Right(s)**" means all patent rights, copyrights, trademark rights, rights in trade secrets (if any), design rights, database rights, domain name rights, moral rights, and any other intellectual property rights (registered or unregistered) throughout the world.

1.12 "**Obligations**" means those obligations that Partner or Google is required to carry out under this Agreement, as set out in Attachment A (those Obligations carried out by Partner being referred to as "**Partner Obligations**" and those Obligations carried out by Google being referred to as "**Google Obligations**", Partner Obligations and Google Obligations collectively being referred to as the "**Obligations**").

1.13 "**Partner Provided Content**" means the Content provided by the Partner as listed in Attachment B.

1.14 "**Personal Information**" means:

(A) any information about an identifiable individual, including names, email addresses, postal addresses, telephone numbers, government identification numbers, financial account numbers, payment card information, credit report information, biometric information, IP addresses, network and hardware identifiers, geolocation information, and 'personal data' within the meaning of the GDPR; and

(B) any information that is not specifically about an identifiable individual but, when combined with other information, may identify an individual.

1.15 "**Privacy Laws**" means: (a) the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (until 25 May 2018); (b) the GDPR (from 25 May 2018); and (c) any other privacy, data security, and data protection laws, directives, regulations, and rules in any jurisdiction applicable to Partner and the services under this Agreement.

1.16 "**Third Party Legal Proceeding**" means any legal proceeding filed by a third party before a court or government tribunal (including any [civil, administrative, investigative or] appellate proceeding).

1.17 "In this Agreement, (A) "**include**" or "**including**" means "including but not limited to" and (B) examples are illustrative and not the sole examples of a particular concept.

2. Term and Termination

2.1 This Agreement will commence on the Effective Date and will remain in force until 31st March 2020 unless terminated earlier.

2.2 Termination for Breach. Either party may immediately terminate this Agreement on written notice if the other party: (i) is in material breach of this Agreement where the breach is incapable of remedy; or (ii) is in material breach of this Agreement where the breach is capable of remedy and fails to remedy that breach within fourteen (14) days after receiving written notice of such breach.

2.3 Termination for Legal Cause. Either party may immediately suspend performance or terminate this Agreement if applicable law or an applicable government or court order prohibits performance.

2.4 Termination for Convenience. Google may terminate this Agreement at any time on written notice to Partner, subject to Section 2.5 (Effects of Termination).

2.5 Effect of Termination. Sections 1 (Definitions), 2.5 (Effects of Termination), 4 (Fees and Payment), 5 (Intellectual Property Rights), 6 (Clearances and Approvals), 7 (Confidentiality ,Publicity, Privacy and Security), 8 (Warranties), 9 (Indemnities), 10 (Limitation of Liability) and 11 (General) will survive termination of this Agreement.

3. Co-Marketing.

3.1 Each party will carry out the activities described in Attachment A (Campaign Details and Obligations).

3.2 The parties will work together to develop and implement any Campaign Materials reasonably required by the parties to fulfill their obligations as set out in Attachment A.

3.3 Each party will obtain the prior written approval from the other in relation to the inclusion of any of the other parties Brand Features or Content featured in its Campaign Marketing.

4. Fees and Payment.

4.1 Any payments due under this Agreement (as set out in Attachment A (Campaign Details and Obligations)) are exclusive of VAT and any other duty or tax, which will (if applicable) be payable at the rate and in the manner from time to time prescribed by law. If either party is required by applicable law to withhold or pay withholding tax on any sum payable under this Agreement, it shall be entitled to deduct these amounts from sums paid to the

other party.

4.2 Each party shall pay to the other party all charges properly due and validly invoiced within 45 days of receipt of the invoice.

4.3 Unless otherwise agreed each party will bear its own costs in meeting its obligations under this Agreement.

5. Intellectual Property Rights.

5.1 Brand Features Licence.

(A) Subject to Partner's compliance with (i) Google Brand Features Guidelines at http://www.google.com/permissions/ (or such other URL as Google may specify), and (ii) this Agreement, Google grants to Partner a non-exclusive, non-sub-licensable, royalty-free, fully-paid, worldwide licence during the Term to use the Google Brand Features solely for the purpose of performing Partner's obligations under this Agreement.

(B) Subject to Google's compliance with (i) any Partner branding guidelines provided by Partner to Google in advance, and (ii) this Agreement, Partner grants to Google and its affiliates a non-exclusive, sublicensable, royalty-free, fully-paid, worldwide licence during the Term to use the Partner Brand Features solely for the purpose of performing Google's obligations under this Agreement.

5.2 Content.

(A) Google grants to Partner a non-exclusive, non-sub-licensable, royalty-free, fully-paid, worldwide licence during the Term to use, distribute, publicly perform and publicly display the Google Provided Content in connection with the Campaign. It is specifically acknowledged and agreed that the Partner will not edit, crop, modify or otherwise produce derivative works of the materials provided by Google to Partner as set out in Attachment B (Content).

(B) Partner grants to Google and its affiliates a non-exclusive, non-sub-licensable, royalty-free, fully-paid, worldwide licence during the Term to use, reproduce, prepare derivative works of, distribute, publicly perform, publicly display and otherwise use the Partner Provided Content in connection with the Campaign as permitted in this Agreement.

5.3 All Intellectual Property Rights developed by a party prior to the Effective Date of this Agreement and all Intellectual Property Rights developed by one party independently of the other party will, as between the parties, remain the sole and exclusive property of that party or that party's licensors.

5.4 Except for the licensed rights under Section 5.1 and 5.2, neither party will own or acquire any right, title, or interest in any Intellectual Property Rights belonging to the other party, or the other party's licensors.

5.5 All goodwill arising from the use by Partner of the Google Brand Features will belong to Google. All goodwill arising from the use by Google of the Partner Brand Features will belong to Partner.

5.6 Ownership of Campaign Materials.

(A) Google owns any Campaign Materials, and any Intellectual Property Rights in the Campaign Materials, except to the extent that it includes the Content.

(B) Google grants a to Partner a non-exclusive, non-sub-licensable, royalty-free, fully-paid, worldwide licence during the Term to use, reproduce, prepare derivative works of, distribute, publicly perform, publicly display and otherwise use the Campaign Materials in connection with the Campaign as permitted in this Agreement.

6. Clearances and Approvals.

6.1 Prior to the beginning of the Campaign Period, each party will obtain or procure any and all third party clearances, approval and/or consents in order to feature its respective Content in the Campaign Materials during the Campaign Period (and for a suitable timeframe beyond the Campaign Period if there are any printed or hard copy materials that would remain in circulation) in accordance with Attachment B (Content).

6.2 Each party will obtain the prior written approval from the other in relation to the inclusion of any of the other party's Brand Features or Content featured in its Campaign.

6.3 Extension of the Campaign Period. The Campaign Period may only be extended subject to each of the parties agreeing to renew clearances (where needed) for their respective Content and being able to obtain such renewed clearances for the extended period.

7. Confidentiality, Publicity, Privacy and Security.

7.1 Confidentiality Obligations**.** The recipient will not disclose the discloser's Confidential Information, except to employees, affiliates, agents or professional advisors ("**Delegates**") who need to know it and who have a legal obligation to keep it confidential. The recipient will use the Confidential Information only to exercise rights and fulfill obligations under this Agreement. The recipient may disclose Confidential Information when legally compelled by a court or other government authority. To the extent permitted by law, recipient will promptly provide the discloser with sufficient notice of all available details of the legal requirement and reasonably cooperate with the discloser's efforts to challenge the disclosure, seek an appropriate protective order, or pursue such other legal action, as the discloser may deem appropriate. The recipient will ensure that its Delegates are also subject to the same non-disclosure and use obligations.

7.2 No Rights. Except for the limited rights under this Agreement, neither party acquires any right, title, or interest in the other party's Confidential Information.

7.3 No Publicity. Neither party may make any public statement regarding this Agreement without the other party's written approval.

7.4 Privacy and Security. If Partner has access to Protected Information (as defined in Attachment C (Information Security)) in connection with this Agreement, then Partner will comply with Attachment C (Information Security).

8. Warranties.

8.1 Mutual. Each party represents and warrants that:

(A) Authority. It has full power and authority to enter into and fulfill its obligations under this Agreement;

(B) License Rights. It has and will retain all necessary rights to grant the licences in this Agreement;

(C) Quality. Performance of its obligations under this Agreement will be performed with reasonable skill and care;

(D) No Breach of Third Party Obligations. Performance of its obligations under this Agreement will not breach any obligations it has to any third party.

8.2 Subject to Section 10.3 (c) no implied conditions, warranties or other terms apply (including any implied terms as to satisfactory quality, fitness for purpose or conformance with description).

8.3 Partner represents and warrants that the Partner Brand Features, Partner Provided Content and Campaign Materials will not violate any applicable law or regulation or contain any material which may be harmful, abusive, obscene, threatening or defamatory.

8.4 Anti-Bribery. Partner will comply with all applicable commercial and public anti-bribery laws, including the U.S. Foreign Corrupt Practices Act of 1977 and the UK Bribery Act of 2010, which prohibit corrupt offers of anything of value, either directly or indirectly to anyone, including government officials, to obtain or keep business or to secure any other improper commercial advantage. "Government officials" include any government employee; candidate for public office; and employee of government-owned or government controlled companies, public international organisations, and political parties. Furthermore, Partner will not make any facilitation payments, which are payments to induce officials to perform routine functions they are otherwise obligated to perform. Partner will use commercially reasonable and good faith efforts to comply with Google's due diligence process, including providing requested information.

8.5 Modern Slavery. Partner will comply with all applicable anti-slavery and human trafficking laws and regulations including the UK Modern Slavery Act 2015.

9. Indemnities.

9.1 Obligations.

(A) Google Obligations. Google will indemnify Partner and its affiliates, directors, officers and employees against all settlement amounts and any liabilities, damages, losses, costs, fees (including legal fees), and expenses in connection with any Third Party Legal Proceeding (including action by a government authority) to the extent arising from any allegations claiming that the Google Provided Content or Google Brand Features infringe or violate any third party's rights, including Intellectual Property Rights.

(B) Partner Obligations. Partner will indemnify Google and its affiliates, directors, officers and employees against all settlement amounts and any liabilities, damages, losses, costs, fees (including legal fees), and expenses in connection with any Third Party Legal Proceeding (including action by a government authority) to the extent arising from any allegations claiming that the Partner Provided Content and Partner Brand Features infringe or violate any third party's rights, including Intellectual Property Rights.

9.2 Exclusions. This Section 9 (Indemnity) will not apply to the extent that the underlying allegation arises from the indemnified party's breach of this Agreement or use of or modifications to the indemnifying party's Content or brand features (as applicable) other

than in accordance with this Agreement.

9.3 Conditions. Section 9.1 (Obligations) is conditioned on the indemnified party:

(A) Promptly notifying the indemnifying party in writing of any allegation(s) that preceded any Third Party Legal Proceeding and cooperating reasonably with the indemnifying party to resolve the allegation(s) and third party claim. If a breach of this Subsection 9.3 (A) prejudices the defence of the third party claim, the indemnifying party's obligations under this Section 9 (Indemnity) will be reduced in proportion to the prejudice.

(B) The indemnified party must tender sole control of the indemnified portion of the Third Party Legal Proceeding to the indemnifying party, subject to the following:

(1) the indemnified party may appoint its own non-controlling legal counsel, at its own expense; and

(2) any settlement requiring the indemnified party to admit liability, pay money, or take (or refrain from taking) any action, will require the indemnified party's prior written consent, not to be unreasonably withheld, conditioned, or delayed.

9.4 Sole Rights and Obligations. Without affecting either party's termination rights, this Section 9 states the parties' only rights and obligations in connection with this Agreement for any third-party Intellectual Property Rights allegations and third party claims.

10. Limitation of Liability.

10.1 Liability. In this Section 10 (Limitations of Liability), "**liability**" means any liability, whether under contract, tort, or otherwise, including for negligence.

10.2 Limitations. Subject to Section 10.3 (Exceptions to Limitations):

(A) Neither party will have any liability arising out of or relating to this Agreement for:

(1) the other party's loss of profit or revenues; or

(2) indirect or consequential losses (whether or not foreseeable or contemplated by the parties at the Effective Date).

(B) Subject to Section 10.2 (A) and (C) each party's aggregate liability arising out of or relating to this Agreement is limited to €10,000 EURO.

(C) Each party's total liability arising under Section 9 (Indemnity) of this Agreement is limited to €500,000 EURO.

10.3 Exceptions to Limitations. Nothing in this Agreement excludes or limits either party's liability for:

(A) death or personal injury resulting from its negligence or the negligence of its employees or agents;

(B) fraud or fraudulent misrepresentation;

(C) breach of any implied condition as to title or quiet enjoyment;

(D) breach of Section 7 (Confidentiality, Publicity, Privacy and Security);

(E) matters for which liability cannot be excluded or limited under applicable law.

11. **General**.

11.1 Notices. All notices of termination or breach must be in English, in writing and addressed to the other party's legal department. All other notices must be in English, in writing and addressed to the other party's primary contact. Notice can be by email and will be treated as given on receipt, as verified by written or automated receipt or by electronic log (as applicable).

11.2 Assignment. Partner may not assign or transfer its rights or obligations under this Agreement, and any attempt to do so is void. Google may assign or transfer any of its rights or obligations under this Agreement to an affiliate.

11.3 Change of Control. During the Term, if Partner experiences a change of control (for example, through a stock purchase or sale, merger, or other form of corporate transaction), then Partner will give written notice to Google within 30 days after the change of control.

11.4 Subcontracting. Either party may subcontract any of its obligations under this Agreement, but will remain liable for all subcontracted obligations and its subcontractors acts or omissions.

11.5 Force Majeure. Neither party will be liable for failure or delay in performance to the extent caused by circumstances beyond its reasonable control.

11.6 No Waiver. Neither party will be treated as having waived any rights by not exercising (or delaying the exercise of) any rights under this Agreement.

11.7 No Agency. This Agreement does not create any agency, partnership, or joint venture between the parties.

11.8 No Third-Party Beneficiaries. This Agreement does not confer any benefits on any third party unless it expressly states that it does.

11.9 Execution. The parties may execute this Agreement using electronic signatures, electronic copies, and counterparts.

11.10 Entire Agreement. Subject to Section 10.3 (B) this Agreement states all the terms agreed between the parties and supersedes all other agreements between the parties as of the Effective Date, relating to its subject matter. In entering into this Agreement neither party has relied on, and neither party will have any right or remedy based on, any statement, representation or warranty (whether made negligently or innocently), except those expressly stated in this Agreement.

11.11 Amendments. Any amendment must be in writing, signed by both parties, and expressly state that it is amending this Agreement.

11.12 Severability. If any term (or part of a term) of this Agreement is invalid, illegal or unenforceable, the rest of this Agreement will remain in effect.

11.13 Conflicting Languages. If this Agreement is translated into any other language, and there is a discrepancy between the English text and the translated text, the English text will govern.

11.14 Governing Law. This Agreement is governed by English law and the parties submit to the exclusive jurisdiction of the English courts in relation to any dispute (contractual or non-contractual) concerning this Agreement save that either party may apply to any court for an injunction or other relief to protect its Intellectual Property Rights.

Signed by the parties' authorised representatives on the dates below.

Partner:	**Google**
By:	**By:**
Name:	**Name:**
Title:	**Title:**
Date:	**Date:**

ATTACHMENT A: CAMPAIGN DETAILS AND OBLIGATIONS

1. CAMPAIGN DETAILS

1.1. The "**Campaign**": Google and Partner are partnering to create a Grow with Google skills and training hub situated at a physical location within the City of Helsinki (the "**Hub**"). The Hub will focus on upskilling users, who will mainly be SMBs, people who are unemployed and other individuals seeking to improve their digital knowledge.

Campaign activities are outlined in this Attachment A.

Provision	Details
Campaign Name	Grow with Google Hub - City of Helsinki
Campaign Description	The Hub will be located at a physical location within the City of Helsinki and will provide skills and training to users, who will mainly be SMBs, people who are unemployed and other individuals seeking to improve their digital knowledge (the "**Trainees**").
Partner Obligations	● Recruit and screen Trainees for programmes run by the Hub, i.e. SMBs, people who are unemployed and other individuals seeking to improve their digital knowledge. ● Provide a Hub host/manager who will work at the Hub full-time during the Campaign Period, and will be a member of the City of Helsinki staff (paid for and managed by the Partner). The Hub host/manager will be responsible for the day-to-day management of the Hub. ● Provide the name and logo of the City of Helsinki to be used at the Hub and on promotional materials for the Hub. ● Run specific promotional activities advertising the Hub to target audiences to include: newsletters, mailings, social media and own media promotion of the Hub and its programmes. ● Provide consultation to Google on the training curriculum as the Partner has the expertise on Trainee needs (jobseekers and SMBs) ● Offer municipal (social and economic) services at the Hub to Trainees and other visitors. For example, jobseekers' support. Such services shall be discussed and agreed with Google from time to time. ● Partner may provide materials related to the municipality's and state's employment and social services. ● Partner will manage the sign up process for individuals taking part in Partner activities (such as provision of jobseekers' support services and Partner events) at the Hub.
Google Obligation	● Develop the Hub at a location in the city centre of Helsinki. Google will be responsible for preparing the agreed site for use as the Hub. This will include, designing, furnishing and equipping the Hub for use (Google will use a sub-contractor for this purpose). ● Provide general maintenance of the Hub for the Campaign Period. ● Provide Grow with Google training materials for use at the Hub. Google will provide the curriculum, training content design and manage the implementation of the training materials.

	● Google will recruit, provide and manage trainers to deliver Grow with Google training at the Hub. ● Google will be responsible for the management of events at the Hub. ● Google shall obtain completed satisfaction and impact surveys from Hub participants during the Campaign Period. ● Google will manage the sign up process for individuals taking part in Google activities (such as Grow with Google training and Google events) at the Hub. ● Google may, at its sole discretion, provide small marketing collateral to the Hub, including pens, pads, stickers etc. ● Google may, at its sole discretion, provide flyers, tabletop displays, and/or brochures for different topics, e.g. safety or privacy or product guides etc. ● Google may, at its sole discretion, obtain support for the Hub from additional partners. Such additional partners may be showcased, for example by: adding the partner's logo to the partners' wall at the Hub; including the logo on relevant marketing materials; including the additional partner on the Google website or online media promoting the Hub; and such other activities/promotions to be decided by Google at its sole discretion.
Partner Deliverables	Newsletters, mailings, social media posts and own media promotion of the Hub and its programmes
Google Deliverables	Google may, at its sole discretion, provide: (i) small marketing collateral to the Hub, including pens, pads, stickers etc; and/or (ii) flyers, tabletop displays, and/or brochures for different topics, e.g. safety or privacy or product guides etc.
Joint Activities and Obligations	Both parties will work together to: (i) agree on marketing channels to promote the Campaign; and (ii) manage and conduct PR and media outreach. Both parties will put on joint events at the Hub, including coordinating 'matchmaking' events between Trainees and SMBs (and such other events as agreed between the parties from time to time). Both parties will be responsible for tracking and reporting on the number of Trainees using the Hub each day.
Fees	None
Campaign Territory	City of Helsinki

ATTACHMENT B: CONTENT

1. Content.

1.1. The table below sets out the responsibility of the parties to provide and clear their respective Content.

Content to be Featured in the Campaign	Responsibility for providing the Content
Newsletters, mailings, social media posts and Partner's own media promotion of the Hub and its programmes.	Partner
Google may, at its sole discretion, provide: (i) small marketing collateral to the Hub, including pens, pads, stickers etc; and/or (ii) flyers, tabletop displays, and/or brochures for different topics, e.g. safety or privacy or product guides etc.	Google

ATTACHMENT C: INFORMATION SECURITY
Dual Role Information Protection Addendum ("DRIPA")

Part A: General Information Security Terms

1. **Introduction**.

1.1 Order of Precedence. Unless otherwise stated in the Agreement, if there is any conflict or inconsistency between this DRIPA and the Agreement, this DRIPA will prevail.

1.2 Supplemental Terms. In addition to this DRIPA Part A (General Information Security Terms), the following supplemental terms are part of the Agreement to the extent applicable:

(a) Part B (EU Data Protection Requirements for Data Processors) of this DRIPA will apply to Services You perform in Your capacity as Data Processor.

(b) Part C (EU Data Protection Terms for Data Controllers) of this DRIPA will apply to Services You perform in Your capacity as Data Controller.

2. **Definitions; Interpretation**.

2.1 Definitions. In this DRIPA :

(a) "**Access**" or "**Accessing**" means to create, collect, acquire, receive, record, consult, use, process, alter, store, maintain, retrieve, disclose, or dispose of. Access also includes "**processing**" within the meaning of EU Data Protection Laws.

(b) "**Applicable Laws**" means all privacy, data security, and data protection laws, directives, regulations, and rules in any jurisdiction applicable to Your access to any Personal Information and the Services.

(c) "**Applicable Standards**" means government standards, industry standards, and best practices applicable to Your access to any Personal Information for the Services including the Privacy Shield.

(d) "**Customer Personal Information**" means Personal Information that the Data Subject uploads or otherwise provides You in connection with its use of Your Services.

(e) **"Data Controller**" has the same meaning as "controller" in EU Data Protection Laws.

(f) "**Data Processor**" has the same meaning as "processor" in EU Data Protection Laws.

(g) **"Data Subject"** has the same meaning as "data subject" in EU Data Protection Laws.

(h) "**EU Data Protection Laws**" means, as applicable: (i) the GDPR; and, (ii) any other applicable data protection laws or regulations modeled on the GDPR.

(i) "**EU Personal Information**" means Personal Information subject to EU Data Protection Laws.

(j) "**includes**" or "**including**" means, "including but not limited to".

(k) "**Personal Information**" means (i) any information about an identified or identifiable individual; or (ii) information that is not specifically about an identifiable individual but, when combined with other information, may identify an individual. Personal Information includes names, email addresses, postal addresses, telephone numbers, government identification numbers, financial account numbers, payment card information, credit report information, biometric information, online identifiers (including IP addresses and cookie identifiers), network and hardware identifiers, and geolocation information. In this Agreement, "Personal Information" includes any information that constitutes "**personal data**" within the meaning of the EU Data Protection Laws.

(l) "**the Privacy Shield**" means the EU-U.S. and Swiss-U.S. Privacy Shield Framework agreements between the United States Department of Commerce and the European Union and Swiss Administration, respectively, that regulates transferring Personal Information from the European Union and Switzerland to the United States.

(m) "**Protected Information**" means Personal Information and Google Confidential Information that You or a Third Party Provider may Access in performing Services. Protected Information does not include the parties' business contact information (specifically, business addresses, phone numbers, and email addresses, including a party's contact persons' names used solely to facilitate the parties' communications for administration of the Agreement).

(n) **"reasonable"** means reasonable and appropriate to (i) the size, scope, and complexity of Your business; (ii) the nature of the Protected Information being Accessed; and (iii) the need for privacy, confidentiality, and security of the Protected Information.

(o) "**Regulator**" or "Regulatory" means an entity with supervisory or regulatory authority over
Google or its affiliate under Applicable Laws.

(p) **"Safeguards"** means the administrative, technical, organizational, and physical controls in Section 5 (Safeguards), Section 6 (Encryption Requirements), Section 8.3 (Your Self-Assessment), and Section 9.1 (Security Incident Response Program).

(p) **"Security Incident"** means actual or reasonable degree of certainty that unauthorized destruction, loss, alteration, disclosure of, or access to, Protected Information for which You are responsible. Security Incidents do not include unsuccessful access attempts or attacks that do not compromise the confidentiality, integrity, or availability of Protected Information, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

(r) **"Services"** means any goods or services that You or a Third Party Provider provide(s) to or for Google either (a) under one or more statements of work (SOW) entered under the Agreement; or (b) if no SOW has been entered under the Agreement, under the Agreement itself.

(s) "**Standard Contractual Clauses**" means the Standard Contractual Clauses (Set II) for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

(t) "**Third Party Provider**" means any parent company, subsidiary, agent, contractor, sub-contractor, sub-processor, or other third party You authorize to act on Your behalf in connection with processing Personal Information exclusively intended for the Services. "**Third Party Provider"** includes "**sub-processor**" within the meaning of Standard Contractual Clauses.

(u) **"You"** or **"Your"** means the party (including any personnel, contractor, or agent acting on behalf of such party) that performs Services for Google or its affiliates under the Agreement.

2.2 Interpretation. All capitalized terms that are not expressly defined in the DRIPA will have the meanings given to them in the Agreement. Any examples in this DRIPA are illustrative and not the sole examples of a particular concept.

2.3 Roles and responsibilities of the Parties.

(a) You Acting as Data Processor. You acknowledge and agree that You are acting as a Data Processor and Google is acting as a Data Controller with respect to Your Access of Personal Information to assist with the day-to-day management of the Hub when You provide a Hub host/manager during the Campaign Period. The Hub manager may assist with handling attendance records for Google, such records may include the names and contact details (email addresses, telephone and postal address) of Hub users; and You will comply with the terms and conditions of this DRIPA identified as applicable to You as Data Processor.

(b) You Acting as Data Controller. You acknowledge and agree that You are acting as an independent Data Controller with respect to Your Access of Customer Personal Information to screen and recruit Hub users and provide municipal (social and economic) services directly to Hub users, as set out in this Agreement; Google is not responsible for any failure by You to comply with Your obligations under EU Data Protection Law relating to Your Access of Personal Information; and You will comply with the terms and conditions of this DRIPA identified as applicable to You as Data Controller**.**

3. Compliance with Laws; Use Limitation; Privacy Notice.

3.1 Compliance with Applicable Laws and Applicable Standards. When You Access Protected Information under the Agreement as Data Processor or Data Controller, You will at all times comply with all Applicable Laws and Applicable Standards, including any requirements applicable to the transfer of Personal Information out of the European Economic Area ("EEA") or Switzerland. You will promptly notify Google if You believe compliance with this DRIPA will interfere with your obligations under Applicable Laws.

3.2 Purpose Limitation. As Data Processor You will Access Protected Information only for the limited and specified purposes stated in the Agreement; and to exercise Your rights and fulfill Your obligations under the Agreement. You are expressly prohibited from Accessing the Protected Information for any other purpose.

3.3 Privacy Notice. To the extent You collect Personal Information from individuals as Data Controller, You will provide a clear and conspicuous privacy notice to such individuals that accurately describes how You Access and protect that information, and that complies with Applicable Laws and Applicable Standards.

4. Third Party Providers Requirements Applicable to You as Data Processor. You may not subcontract the performance of any part of the Services to any Third Party Provider without Google's prior written consent or general written authorization. If and to the extent Google gives prior consent, You will:

(a) carry out adequate due diligence of Your Third Party Provider to ensure its capability of providing the level of protection for Protected Information required by the Agreement.

(b) contractually require Your Third Party Provider to protect the Protected Information using at least the same level of protection required of You under this Agreement.

(c) retain oversight of and be responsible for Your Third Party Providers' acts and omissions in connection with this Agreement.

(d) You will send any requests for Google's consent to the subcontracting of any part of the Services to a Third Party Provider to subprocessor-compliance@google.com or complete the external webform, Sub-Processing Notifications (https://sites.google.com/corp/view/subprocessor-notifications/home).

5. **Safeguards Applicable to You as Data Processor or Data Controller.** Whether as Data Processor or Data Controller, at all times that You Access Protected Information, You will maintain reasonable technical, organizational, administrative, and physical controls and comply with this DRIPA , Applicable Standards, and Applicable Laws, including the following:

(a) Physical Controls. You will maintain physical Access controls designed to secure relevant facilities, including layered controls covering perimeter and interior barriers, individual physical access controls, strongly-constructed facilities, suitable locks with key management procedures, access logging, and intruder alarms/alerts and response procedures.

(b) Logical Controls**.** To the extent You Access Protected Information using Your systems, You will:

(i) establish and enforce access control policies and measures to ensure that only individuals who have a legitimate need to Access Protected Information will have such access, including multi-factor authentication;

(ii) promptly terminate an individual's access to Protected Information when such access is no longer required for performance under the Agreement;

(iii) maintain reasonable and up-to-date anti-malware, anti-spam, and similar controls on Your networks, systems, and devices;

(iv) log the appropriate details of access to Protected Information on Your systems and equipment, plus alarms for attempted access violations, and retain such records for no less than 90 days;

(v) maintain controls and processes designed to ensure that all operating system and application security patches are installed within the timeframe recommended or required by the issuer of the patch; and

(vi) implement reasonable user account management procedures to securely create, amend, and delete user accounts on networks, systems, and devices through which You Access Protected Information, including monitoring redundant accounts and ensuring that information owners properly authorize all user account requests.

(c) Personnel Security. You will maintain personnel policies and practices restricting access to Protected Information, including having written confidentiality agreements and performing background checks in accordance with Applicable Laws on all personnel who Access Protected Information or who maintain, implement, or administer Your Safeguards.

(d) Training and Supervision. You will provide reasonable ongoing privacy and information security training and supervision for all Your personnel who Access Protected Information.

6. **Encryption Requirements.** Using a reasonable encryption standard, You will encrypt all Protected Information that is (a) stored on portable devices or portable electronic media; (b) maintained outside of Google's or Your facilities; or (c) transferred across any telecommunications network not solely managed by You; and (d) where required by Applicable Law, including Personal Information at rest on Your systems.

7. **Use of Google Networks, Systems, or Devices Requirements Applicable to You as Data Processor or Data Controller**. To the extent that You access Google-owned or Google-managed networks, systems, or devices (including Google APIs, corporate email accounts, equipment, or facilities) to Access Protected Information, You agree to comply with Google's written instructions, system requirements, and policies made available to You.

8. **Assessments of Data Processors; Audits; Corrections Requirements Applicable to You as Data Processor or Data Controller**.

8.1 Google's Security Assessment. On Google's written request You will promptly and accurately complete Google's written information privacy and security questionnaire regarding any network, application, system, or device, or Safeguard applicable to Your access to the Protected Information. You will provide any additional assistance and cooperation that Google may reasonably require during any assessment of Your Safeguards, including providing Google with reasonable access to personnel, information, documentation, infrastructure and application software, to the extent any of the foregoing is involved in Your access to the Protected Information.

8.2 Penetration Testing. If You Access Protected Information on Your systems as a Data Processor, or Your systems connect to Google's internal systems, then in addition to Section 8.1 (Google's Security Assessment), the following will apply:

(a) Google Conducted Penetration Test. Upon reasonable notice, in coordination with You (or Google's independent third party assessor that is not Your competitor) Google may perform annual penetration testing or other security assessment on Your systems used to Access Protected Information. Google reserves the right to perform more frequent testing in connection with material changes to Services, or as a result of any Material Vulnerability or Security Incident notified to Google.

(b) Third Party Conducted Penetration Test. Instead of a Google-conducted penetration test under Section 8.2(a), at Google's sole discretion, Google may accept the written results of penetration testing (and the status of Your efforts to remediate findings, if any) performed by Your accredited third party vulnerability tester following commonly accepted guidelines consistent with Google's then current Testing Guidelines (https://partner-security.withgoogle.com/docs/pentest_guidelines). Google will treat the information You disclose in connection with Section 8 as Your confidential information.

8.3 Your Continuous Self-Assessment. You will continuously monitor risk to the Protected Information and ensure that the Safeguards are properly designed and maintained to prevent unauthorized access to the Protected Information. You will periodically (but no less than once per year) ensure third party penetration tests and other appropriate vulnerability tests are conducted, and document the effectiveness of Your Safeguards.

8.4 Audits and Certifications; Supervisory Authority Audit. Where You Access Personal Information as a Data Processor the following will apply:

(a) Audits and Certifications. Upon written request by Google, not more than once per year, Google may conduct an audit of Your architecture, systems and procedures relevant to the protection of Personal Information at locations where Personal Information is Accessed. You will work cooperatively with Google to agree on an audit plan in advance of any audit. Provided, however, if the scope of the audit is addressed in a SSAE 16/ISAE 3402 Type 2, ISO, NIST, PCI DSS, HIPAA or similar audit report performed by a qualified third party auditor within the prior twelve (12) months, and You confirm there are no known material changes in the controls audited, Google may agree to accept those reports in lieu of requesting an audit of the controls covered by the report.

(b) Supervisory Authority Audit. Notwithstanding Section 8.4(a), if a Regulator requires an audit of the data processing facilities from which You processes Personal Information in order to ascertain or monitor Google's compliance with EU Data Protection Law, You will cooperate with such audit.

8.5 Correcting Vulnerabilities. If either party discovers that Your Safeguards contain a vulnerability, You will promptly correct or mitigate at Your own cost (a) any vulnerability within a reasonable period, and (b) any material vulnerability within a period not to exceed 60 days. If Google identifies the vulnerabilities, You will provide Google with reasonable assurances that Your corrections meet this DRIPA 's requirements. If You are unable to correct or mitigate the vulnerabilities within the specified time period, You must promptly notify Google and propose reasonable remedies. Compliance with this DRIPA Section will not reduce or suspend Your obligations under Section 9 (Security

Incident Response), or reduce or suspend Google's rights under Section 12 (Suspension; Termination), and 13 (Records; Destruction; Sanitization).

9. **Security Incident Response Requirements Applicable to You as Data Processor.**

9.1 Security Incident Response Program. You will maintain a reasonable Security Incident response program.

9.2 Security Incident Notification.

(a) If You become aware of a Security Incident, You will promptly:

(i) stop the unauthorized access;

(ii) secure the Protected Information;

(iii) notify Google (in no event more than 24 hours after discovery of the Security Incident) by sending an email to *external-incidents@google.com* with the information described in Subsection (b) below; and

(iv) assist Google in ensuring compliance with its Security Incident notification obligations under Applicable Laws and as otherwise reasonably requested.

(b) You will provide reasonable information about the Security Incident, including:

(i) a description of the Protected Information subject to the Security Incident (including the categories and number of data records and Data Subjects concerned) and the likely consequences of the Security Incident;

(ii) the date and time of the Security Incident;

(iii) a description of the circumstances that led to the Security Incident (e.g., loss, theft, copying);

(iv) a description of the measures You have taken and propose to take to address the Security Incident; and

(v) relevant contact people who will be reasonably available until the parties mutually agree that the Security Incident has been resolved. For Security Incidents involving Personal Information, "reasonably available" means 24 hours per day, 7 days per week.

9.3 Remediation; Investigation. At Your cost, You will take appropriate steps to promptly remediate the root cause(s) of any Security Incident, and will reasonably cooperate with Google with respect to the investigation and remediation of such incident, and provide such assistance as required to enable Google to satisfy its obligation to notify. You will promptly provide Google the results of the investigation and any remediation already undertaken.

9.4 No Unauthorized Statements. Except as required by Applicable Laws, You will not make (or permit any third party to make) any statement concerning the Security Incident that directly or indirectly references Google, unless Google provides its explicit written authorization.

10. **Legal Process Requirements Applicable to You as Data Processor.** If You or anyone to whom You provide access to Protected Information becomes legally compelled by a court or other government authority to disclose Protected Information, then to the extent permitted by law, You will promptly inform Google of any request and reasonably cooperate with Google's efforts to challenge the disclosure, seek an appropriate protective order, or pursue such other legal action as Google may deem appropriate. Unless required by Applicable Laws, You will not respond to such request, unless Google has authorized You to do so.

11. **PCI Compliance Applicable to You as Data Processor.** To the extent You receive, process, transmit, or store any Cardholder Data for or on behalf of Google, You will at all times meet or exceed all Applicable Laws and Applicable Standards related to the collection, storage, accessing, and transmission of such data, including those established by Payment Card Industry Data Security Standards. "**Cardholder Data**" means any primary account number, cardholder name, expiration date and/or service code, and security-related information (including but not limited to card validation codes/values, full track data, PINs and PIN blocks) used to authenticate cardholders or authorize payment card transactions.

12. **Suspension; Termination Applicable to You as Data Processor or Data Controller.** In addition to Google's suspension and termination rights in the Agreement, Google may: (a) immediately suspend Your access to Protected Information if Google reasonably determines that You are not complying with this IPA or Applicable Law; or (b) Google may terminate the Agreement if (i) Google reasonably determines that You have failed to cure material noncompliance with this IPA within a reasonable time; or (ii) Google reasonably believes it needs to do so to comply with Applicable Laws or Applicable Standards.

13. **Records; Destruction; Sanitization. Applicable to You as Data Processor.**

13.1 Records. You will keep at Your normal place of business detailed, accurate, and up-to-date records relating to Your access to Protected Information and sufficient to meet your obligations under this DRIPA . You will make such records available to Google on request.

13.2 Return or Deletion of Information. Upon the termination or expiration of the Agreement or the relevant statement of work for the Services, You will promptly return to Google all copies, whether in written, electronic or other form or media, of Personal Information in Your possession or the possession of Third Party Provider; where permitted delete and render the Protected Information unreadable in the course of disposal, securely dispose of all such hard copies, and where requested certify in writing to Google Your compliance.

13.3 Sanitization. You will use a media sanitization process that deletes and destroys data in accordance with the US Department of Commerce's National Institute of Standards and Technology's guidelines in NIST Special Publication 800-88 or equivalent standard.

14. **Survival. Applicable to You as Data Processor or Data Controller.** Your obligations under this DRIPA will survive expiration or termination of the Agreement and completion of the Services as long as You continue to have access to Protected Information.

Part B: Processing of EU Personal Information Applicable to You as Data Processor

1. **Introduction**. This Part B will only apply to the extent Your Services requires You to Access EU Personal Information.

2. **Types and Categories of Personal Information**. The purchase order(s) or statement(s) of work associated with the Services will specify the subject matter and duration of the processing, the categories of Data Subjects, and the types and categories of Personal Information Accessed.

3. **Roles and Responsibilities**

3.1 If EU Data Protection Laws apply to the Services, the parties acknowledge and agree that:

(a) the subject matter and details to the processing are as described in the Agreement;

(b) Google or its affiliate is a controller of the Personal Information;

(c) You are a processor of the Personal Information; and

(d) You will comply with Google's written instructions with respect to the Personal Information.

3.2 Your Obligations as a Data Processor. You will:

(a) Access Personal Information only on behalf of Google and in accordance with Google's documented instructions unless You are otherwise required by EU Data Protection Law, in which case You will inform Google of that legal requirement before Accessing the Personal Information, unless informing Google is prohibited by law on important grounds of public interest. You will immediately inform Google if, in Your opinion, Google's instructions infringe EU Data Protection Law;

(b) implement and maintain appropriate technical and organizational measures to meet Your obligations under Applicable Laws and this DRIPA ;

(c) promptly correct, amend, or delete the Personal Information at Google's direction;

(d) where requested, reasonably assist Google in the conduct of data protection impact assessments and prior consultations with Regulatory Authorities or other competent data privacy authorities, which Google reasonably considers to be required prior to Accessing Personal Information;

(e) not appoint or change any Sub-Processor without Google's prior written consent, which Google will grant or deny without unreasonable delay, and if granted, You will enter into a contract with each new Sub-Processor in accordance with Part A, Section 4(b) of this DRIPA;

(f) on request, provide Google with information about any authorized Sub-Processor, including a summary or copy of Your contractual terms with such parties, if required by Applicable Laws;

(g) promptly notify Google of any Data Subjects' request to exercise their legal rights or to access, correct, amend, delete, or restrict that person's Personal

Information, to object to the Accessing of Personal Information or exercise the right to data portability in respect of Personal Information.Provided, however, You will not respond to such requests without Google's prior written consent;

(h) cooperate with and assist Google in investigating Data Subjects' exercise of their legal rights;

(i) appoint a Data Protection Officer if legally required, and notify Google of the Data Protection Officers contact information on Google's request; and

(j) maintain adequate records of processing activities as set out more fully in Art. 30 of the GDPR.

4. **Data Transfers.**

4.1. Transfers of Data Out of the European Economic Area and Switzerland. Either party may transfer EU Personal Information outside the European Economic Area and Switzerland if it complies with the provisions on the transfer of personal data to third countries in EU Data Protection Laws.

4.2 Transfers Under Privacy Shield.

(a) Google LLC is certified under Privacy Shield on behalf of itself and certain of its wholly-owned U.S. subsidiaries. Privacy Shield will apply to the transfer of EU Personal Information from the EU and Switzerland to the US. Google's certification is at https://www.commerce.gov/page/eu-us-privacy-shield.

(b) To the extent You will Access EU Personal Information transferred to Google in reliance on Google's Privacy Shield certification, You will:

(i) provide at least the same level of protection for the EU Personal Information as is required by the Privacy Shield for as long as You Access the EU Personal Information; and

(ii) promptly notify Google in writing if You determine that You can no longer provide at least the same level of protection for the EU Personal Information as is required by the Agreement and applicable Privacy Shield principles and, upon making such a determination, cease Accessing the EU Personal Information or take other reasonable and appropriate remediation steps.

4.3. Transfers Under Standard Contractual Clauses. To the extent Standard Contractual Clauses are applicable to the transfer of EU Personal Information from the EU and Switzerland, You expressly agree that the Standard Contractual Clauses will apply to the Services, and Your signature on the Agreement will be treated as Your acceptance of the Standard Contractual Clauses.

4.4 Order of Precedence. In the event that Services are covered by more than one transfer mechanism, the transfer of Personal Information will be subject to a single transfer mechanism in accordance with the following order of precedence:

(a) Privacy Shield
(b) Standard Contractual Clauses

Part C: Processing of EU Personal Information Applicable to You as Data Controller

1. **Introduction**. To the extent You Access Customer Personal Information subject to the GDPR, as Data Controller, the following terms and conditions in this DRIPA Part C will apply.

2. Receiving Data Controller. To the extent You Access Customer Personal Information as Data Controller, You will:

(a) be an independent Data Controllers with respect to the Customer Personal Information Accessed under this Agreement;

(b) individually determine the purposes and means of its processing of the Customer Personal Information;

(c) provide Data Subjects with a clear and conspicuous privacy notice and opportunity to choose, in a manner that complies with EU Data Protection Laws; and

(d) provide individuals with rights in connection with Customer Personal Information, including the ability: (i) to access the Customer Personal Information held about them; and (ii) to correct, amend, or delete that information where it is inaccurate, or has been Accessed in violation of Applicable Laws

3. Data Transfers.

3.1. Transfers of Data Out of the European Economic Area and Switzerland. If You transfer Customer Personal Information to a third country outside the European Economic Area and Switzerland, You will comply with the provisions on the transfer of personal data to third countries.

3.2 Transfers under Privacy Shield.

(a) Google LLC is certified under Privacy Shield on behalf of itself and certain of its wholly-owned U.S. subsidiaries. Privacy Shield will apply to the transfer of EU Personal Information from the EU and Switzerland to the US. Google's certification is at https://www.commerce.gov/page/eu-us-privacy-shield.

(b) To the extent You will Access Personal Information transferred to Google in reliance on its Privacy Shield certification, You will:

(i) provide at least the same level of protection for the Personal Information as is required by Article 3(a) of the Privacy Shield for as long as You Access the Personal Information; and

(ii) promptly notify Google in writing if You determine that You can no longer provide at least the same level of protection for the Personal Information as is required by the Agreement and applicable Privacy Shield principles and, upon making such a determination, cease Accessing the Personal Information or take other reasonable and appropriate remediation steps.

3.3. Acceptance of the Standard Contractual Clauses. To the extent they are applicable, the accessing party expressly agrees to enter into the Standard Contractual Clauses without delay.